и политике «Know your customer». Подавляющее большинство банков намерены использовать биометрические данные в ближайшем будущем.

По мере развития информационных технологий, связанных с использованием биометрических данных в телефонах, существуют правовые проблемы. Связаны данные проблемы в первую очередь с отсутствием полноценной нормативной правовой базы для широкого внедрения биометрических технологий. Заграничный и отечественный опыт внедрения биометрических технологий показал, что у них есть не только сторонники, но и яростные противники, считающие эти технологии средством построения общества тотального контроля и нарушением гражданских свобод. Противники использования биометрических и связанных с ними информационных технологий выражают обеспокоенность по поводу того, как будет использована эта информация, не будут ли нарушаться естественные права граждан на приватность и конфиденциальность.

УДК 004.58; 159.9.01

В. О. Моторина
Научный руководитель: канд. пед. наук, доц. Е. Н. Полякова
Курганский государственный университет, Курган

МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ В ОБЕСЕПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

Аннотация. В данной статье рассмотрено понятие «социальная инженерия». Информация является одним из наиболее ценных ресурсов организации и наиболее уязвимым звеном в потери ценной информации (искажении и т. д.) является человек, которым можно управлять, манипулировать. В данной работе рассмотрены методы атак социальной инженерии и меры противодействия им.

Ключевые слова: атака; метод; социальная инженерия; меры противодействия; угрозы; человеческий фактор.

Правовое обеспечение и сопровождение большинства вопросов в любой организации независимо от формы и вида организации и учреждения — важная составляющая существования и жизнедеятельности организации, начиная от поиска соискателя на вакантную должность в организации и завершая фазой увольнения сотрудника (по собственному желанию или по факту нарушения последним законодательных актов) и прекращения действия в этом случае трудового договора или контрактного договора с лицом вступившего в договорные отношения с организацией.

© Моторина В. О., 2017

К сожалению, сегодня специалисту по защите информации приходится быть ко всему прочему и хорошим юристом, чтобы максимально грамотно подходить к вопросам, которые попадают в поле его компетенции и непосредственной деятельности. Причиной такому положению вещей являются условия формирования законодательной базы, так как ее нельзя сегодня назвать сложившейся или сформировавшийся в виду массы неопределенностей и неоднозначности трактовок как таковых по ряду ключевых определений и несостоятельности однозначно разрешать возникающие вопросы в области информационной безопасности и защите информации в целом.

При формировании локальных актов компании специалист по защите информации использует следующие нормативно-правовые документы:

1. Кодекс РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ.

2. Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ.

3. Уголовный кодекс РФ от 13.05.96 № 63-ФЗ.

4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

6. Указ Президента Российской Федерации от 06.03.97 № 188 «Об утверждении перечня сведений конфиденциального характера».

7. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Какой бы отличной ни была программно-аппаратная защита, всегда остается в уязвимости человек. По данным статистики, среди удачных взломов информационных систем 80 % приходится на использование социальной инженерии.

Социальная инженерия — метод получения необходимого доступа к информации, основанный на особенностях психологии людей [1]. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам. Термин социальной инженерии появился не так давно, а сам метод получения информации таким способом используется довольно долго.

Для того чтобы обезопасить себя от воздействия социальной инженерии, необходимо понять, как она работает. Рассмотрим основные типы социальной инженерии и методы защиты от них.

Претекстинг — это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон и т. п.

Фишинг — техника интернет-мошенничества, направленная на получение конфиденциальной информации пользователей, — авторизационных данных различных систем. Основным видом фишинговых атак является поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме содержится форма для ввода персональных данных (пин-кодов, логина и пароля и т. п.) или ссылка на web-страницу, где располагается такая форма.

Троянский конь — это техника основывается на любопытстве, страхе или других эмоциях пользователей.

Кви про кво (услуга за услугу) — данная техника предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону с просьбой решения какой-либо проблемы, в процессе разговора злоумышленник получает персональные данные или секретную информацию.

Дорожное яблоко — этот метод представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флеш-накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников, туалеты).

Обратная социальная инженерия — данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратится к злоумышленнику за «помощью».

Основным способом защиты от методов социальной инженерии является обучение сотрудников. Все работники компании должны быть предупреждены об опасности раскрытия персональной информации и конфиденциальной информации компании, а также о способах предотвращения утечки данных. Кроме того, у каждого сотрудника компании, в зависимости от подразделения и должности, должны быть инструкции о том, как и на какие темы можно общаться с собеседником, какую информацию можно предоставлять для службы технической поддержки, как и что должен сообщить сотрудник компании для получения той или иной информации от другого сотрудника.

Кроме этого, можно выделить следующие правила:

- пользовательские учетные данные являются собственностью компании;
- необходимо проводить вступительные и регулярные обучения сотрудников компании, направленные на повышения знаний по информационной безопасности;
- обязательным является наличие регламентов по безопасности, а также инструкций, к которым пользователь должен всегда иметь доступ. В инструкциях должны быть описаны действия сотрудников при возникновении той или иной ситуации;

– на компьютерах сотрудников всегда должно быть актуальное антивирусное программное обеспечение;
– в корпоративной сети компании необходимо использовать системы обнаружения и предотвращения атак;
– все сотрудники должны быть проинструктированы, как вести себя с посетителями;
– необходимо максимально ограничить права пользователя в системе.

Исходя из всего перечисленного, можно сделать вывод: основной способ защиты от социальной инженерии — это обучение сотрудников. Необходимо знать и помнить, что незнание не освобождает от ответственности. Каждый пользователь системы должен знать об опасности раскрытия конфиденциальной информации и знать способы, которые помогут предотвратить утечку. Предупрежден — значит, вооружен! [2]

Список литературы

1. *Моторина В. О.*, *Полякова Е. Н.* Манипуляция обществом методами социальной инженерии // Наука и молодежь в XXI веке : сб. науч. тр. студентов и молодых ученых / редкол. В. Г. Роговая, С. В. Косовских. Вып. 13. Курган : Курган. филиал ОУП ВО «АТиСО», 2017. С. 290–294.
2. Хабрахабр [Электронный ресурс]. URL: https://habrahabr.ru/post/83415/.

УДК 004.4

А. Е. Гаращенко
Научный руководитель: ст. преп. Т. И. Паюсова
Тюменский государственный университет, Тюмень

АТРИБУЦИЯ ПРОГРАММНОГО КОДА С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация. В данной работе рассматривается возможность атрибуции программного кода для языка программирования Python с использованием данных, полученных из открытых репозиториев. В статье описываются используемые алгоритмы и инструменты для атрибуции кода с точностью в 73 % среди 50 программистов.

Ключевые слова: информация; безопасность; атрибуция; вредоносный код; авторские права; машинное обучение; Python.

© Гаращенко А. Е., 2017